Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

MANAJEMEN RISIKO SERANGAN SIBER MENGGUNAKAN FRAMEWORK NIST CYBERSECURITY DI UNIVERSITAS ZXC

Tony Tan[1], Benfano Soewito[2],
Program Studi Magister Teknik Informatika[1],
Program Studi Magister Teknik Informatika[2],
Fakultas Teknik Informatika[1], Fakultas Teknik Informatika[2]
Universitas Bina Nusantara[1], Universitas Bina Nusantara[2],

Email: tony.tan@binus.ac.id[1], bsoewito@binus.edu[2],

Received: Febuary 21, 2022**. Revised:** March 17, 2022**. Accepted:** April 05, 2022**. Issue Period:** Vol.6 No.2 (2022), Pp.411-422

Abstrak: Pendidikan tinggi pada saat ini telah menggunakan sistem teknologi informasi seperti sistem layanan berbasis web dan situs web sebagai sarana untuk mendukung pelaksanaan pendidikan. Oleh karena itu, sistem teknologi informasi yang terdapat pada kampus harus terjaga keamanan dan ketahanannya guna untuk memberikan pelayanan yang terbaik untuk dosen, staf, dan mahasiswa. Tidak menutup kemungkinan, sistem teknologi informasi yang terdapat pada kampus memiliki cela peretasan yang bisa dimasuki oleh penjahat dunia maya atau hacker. Oleh karena itu, perlu adanya metode untuk meningkatkan keamanannya. Dalam studi ini, kami menguji keamanan siber pada Universitas ZXC dengan menggunakan Framework NIST Cybersecurity. Pengambilan data dilakukan dengan cara wawancara, studi dokumentasi insiden, dan observasi. Penilaian terhadap 39 sistem layanan web dan situs web. Penulis juga menggunakan aplikasi *Nessus* untuk menilai cela dan tingkat ancaman. Hasil dari penilaian menunjukan hasil kondisi keamanan siber di lingkungan Universitas ZXC masih belum mencapai standar yang direkomendasikan. Hal serupa juga ditunjukan melalui hasil penilaian aplikasi *Nessus* yang menunjukan kondisi cela pada sistem layanan web dan situs web yang cukup banyak. Dari hasil penelitian ini, kami memberikan rekomendasi control menggunakan Framework NIST Cybersecurity untuk meningkatkan keamanan siber pada sistem layanan web dan situs web.
Kata kunci: Serangan Siber; Manajemen Siber; NIST; NIST Cybersecurity Framework;

Abstract: *Higher education currently uses information technology systems such as web-based service systems and websites to support the implementation of education. Therefore, the information technology system on campus must be secure and robust to provide the best service for lecturers, staff, and students. It is possible that the information technology system on campus has hacking flaws that can be entered by cybercriminals or hackers. Therefore, it is necessary to have a method to improve its security. In this study, we tested cybersecurity at ZXC University using the NIST Cybersecurity Framework. Data were collected by means of interviews, incident documentation studies, and observation. Assessment of 39 web service systems and websites. The author also uses the Nessus application to assess flaws and threat levels. The results of the assessment show that the results of cybersecurity conditions in the ZXC University environment have not yet reached the recommended standards. The same thing is also shown through the results of the Nessus application assessment which shows several flaws in the web service system and website. From the results of this study, we provide control recommendations using the NIST Cybersecurity Framework to improve cyber security on web service systems and websites.*
Keywords: *Cybersecurity; Cybersecurity Management; NIST; NIST Cybersecurity Framework*

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

I. PENDAHULUAN

Pendidikan tinggi memiliki karakteristik yang sangat berbeda dengan pendidikan dasar. Secara umum, pelaksanaan pendidikan ditingkat ini membutuhkan sumber daya yang lebih kompleks karena struktur pendidikannya yang berbasis pada penelitian dan industri terbarukan. Untuk mendukung pelaksanaan pendidikan yang luas seperti itu, infrastruktur dan aset IT pada kampus merupakan hal yang sangat penting bagi sistem Teknologi Informasi untuk memberikan layanan untuk staff dan mahasiswa. Selain itu, karena perkembangan teknologi yang mengharuskan kegiatan operasional dilakukan dengan bantuan internet, kebutuhan akan transmisi yang aman dan cepat sangat dibutuhkan untuk produktivitas operasional pada institusi modern, termasuk institusi pendidikan tinggi. Oleh karena itu, infrastruktur jaringan kampus harus terjaga ketahanan, ketersediaan, dan keamanannya.

Salah satu isu terkait penyediaan layanan transmisi data adalah keamanan transmisi data itu sendiri. Studi sebelumnya sudah banyak menjelaskan mengenai pentingnya keamanan pada sistem layanan web dan situs web. Meskipun sudah banyak perkembangan teknologi untuk mendukung keamanan sistem layanan web dan situs web, tidak menutup kemungkinan, sistem layanan web dan situs web yang dibangun pasti memiliki cela yang terbuka yang terdapat pada port dan sistem layanan web. Hal ini menyebabkan masuknya para penjahat dunia maya atau yang dikenal dengan *cybercriminal* untuk menyerang sistem layanan web dan situs web.

Universitas ZXC adalah salah satu Universitas yang ada di Batam yang berdiri sejak tahun 2000. Universitas ZXC memiliki infrastruktur jaringan yang cukup kompleks yang digunakan untuk memberikan layanan kepada staff dan mahasiswa. Yang menjadi permasalahan pada infrastruktur jaringan Universitas ZXC adalah, terdapat beberapa sistem layanan web internal seperti SIA (Sistem Informasi Akademik), dan sistem Portal staff dan mahasiswa pernah diretas sehingga sistem mengalami kegagalan seperti tampilan web services SIA (Sistem Informasi Akademik) dan Portal staff dan mahasiswa Universitas mengalami perubahan. Hal ini menyebabkan terganggunya aktivitas para staff dan juga mahasiswa pada Universitas ZXC untuk beberapa hari. Berdasarkan uraian permasalahan diatas, dapat disimpulkan bahwa sistem layanan web dan situs web pada Universitas ZXC harus dilakukan penanganan terhadap serangan siber.

Menurut Alanda et al [1] untuk melakukan pencegahan terjadinya serangan siber, harus melakukan penetration testing terlebih dahulu agar mendapatkan informasi tentang cela mana saja yang dapat dimasuki oleh cyber criminal. Setelah melakukan penetration testing, disarankan dapat merancang manajemen risiko terhadap serangan siber dengan menggunakan Cybersecurity Framework yang sesuai dengan kebutuhan. Menurut Kohnke et al [2], dengan Cybersecurity Framework, tata kelola terhadap serangan siber menjadi lebih teratur dan efektif dalam menangani risiko serangan siber.

Terdapat banyak cybersecurity framework yang dapat digunakan. Akan tetapi, penulis merekomendasikan menggunakan NIST Cybersecurity Framework yang dirilis oleh National Institute of Standart and Technology (NIST), dan NIST Special Publication 800-53. Framework ini memberikan panduan bagaimana cara mengurangi risiko dan meningkatkan keamanan siber. Selain itu, terdapat beberapa keuntungan menggunakan framework ini, seperti mudah untuk digunakan, dan bisa menghemat biaya pengeluaran dengan cara memilih proses yang paling sesuai dengan kebutuhan pada perusahaan [3][4][5][6]. Dengan melakukan penetration testing dan dan menggunakan framework NIST Cybersecurity, penulis berharap dapat meminimalisir dan meningkatkan keamanan siber disetiap sistem layanan web dan situs web Universitas ZXC.

II. METODE DAN MATERI

2.1. Cybersecurity

Pada era perkembangan teknologi informasi saat ini, keamanan merupakan hal penting yang menjadi konsentrasi atau fokus utama dari penyedia layanan. Hal ini dikarenakan setiap layanan menyimpan informasi penggunaan yang bersifat rahasia. Informasi tersebut dapat berupa nama, tanggal lahir , tempat lahir, nomor handphone,dll. Untuk itu informasi tersebut harus dijaga oleh penyedia layanan agar tidak disalah gunakan oleh orang yang tidak bertanggung jawab [7].

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

2.2. NIST Cybersecurity Framework

NIST Cybersecurity Framework pertama kali dirancang oleh U.S National Institute of Standards and Technology (NIST). Framework ini bertujuan untuk memberikan langkah-langkah mengimplementasikan atau meningkatkan program *cybersecurity* yang ada pada organisasi. Framework ini digunakan untuk melakukan deteksi, mitigasi, dan respon terhadap serangan siber pada organisasi. Framework NIST Cybersecurity mudah untuk digunakan karena Framework ini menggunakan bahasa yang untuk mudah dimengerti. Framework ini juga dapat digabungkan dengan mitigasi risiko serangan siber yang sudah ada sebelumnya pada suatu organisasi. Di dalam inti Framework NIST, terdapat informasi mengenai fungsi, kategori, sub kategori, dan informasi referensi yang dapat dipahami dengan mudah untuk menggunakan Framework ini. Framework ini juga memberikan informasi yang efektif dan mudah untuk memahami struktur, yang terdiri dari Core, Tiers, dan Profil[8]. Core yang terdapat pada Framework NIST Cybersecurity berfungsi untuk memberikan informasi mengenai rekomendasi praktik dari cybersecurity, teknis, hasil, operasional, dan manajemen kontrol. Tiers berfungsi sebagai penilaian terhadap manajemen cybersecurity yang sudah ada pada organisasi. Fungsi Profil pada Framework ini berfungsi untuk mengetahui situasi cybersecurity yang ada pada saat ini dan target cybersecurity yang ingin dicapai oleh organisasi. Dengan menggabungkan ketiga elemen ini, diharapkan dapat membantu organisasi untuk mencapai target dan meningkatkan keamanan siber yang sesuai dengan kebutuhan organisasi.

Berikut ini adalah penjelasan singkat mengenai inti dari Framework NIST Cybersecurity:

- **Functions** berfungsi untuk membantu organisasi dalam melakukan manajemen risiko serangan siber. Kelima fungsi tersebut adalah Identify, Protect, Detect, Respond, dan Recover.
- **Categories** merupakan bagian yang terdapat pada Functions yang berfungsi untuk mewakili aspek keamanan siber.
- **Subcategories** merupakan pernyataan yang diberikan guna untuk pertimbangan atau untuk meningkatkan program keamanan siber. Subcategories merupakan tingkat yang terdalam yang terdapat pada inti Framework yang terdiri dari hasil spesifik dari teknis atau manajerial.
- **Informative Reference** adalah referensi yang berfungsi untuk membantu inti framework guna untuk mencapai hasil atau target yang dijelaskan pada subkategori.

Terdapat lima fungsi yang ada pada inti Framework yaitu:

- **Identify** - Fungsi dari identify adalah untuk membantu mengidentifikasi seluruh aset IT yang terdapat pada organisasi tersebut supaya lebih mudah untuk melakukan cybersecurity management.
- **Protect** - Fungsi dari protect yaitu untuk melakukan proteksi terhadap aset IT yang terdapat pada organisasi sehingga dapat meminimalisir potensi cyber attacks.
- **Detect** - Pada tahap ini, organisasi melakukan pemantauan terhadap aktivitas yang terjadi pada infrastruktur IT agar dapat mengetahui lebih cepat jika terjadi aktivitas yang tidak normal pada infrastruktur IT.
- **Respond** - Fungsi dari respond yaitu ketika terjadi kerusakan pada aset TI, organisasi harus melakukan tindakan yang tepat untuk meminimalisir kerusakan tersebut.
- **Recovery** - Pada tahap recovery, organisasi melakukan pemulihan terhadap kerusakan aset IT akibat cyber attacks agar dapat beroperasi seperti semula.

2.3. Nessus

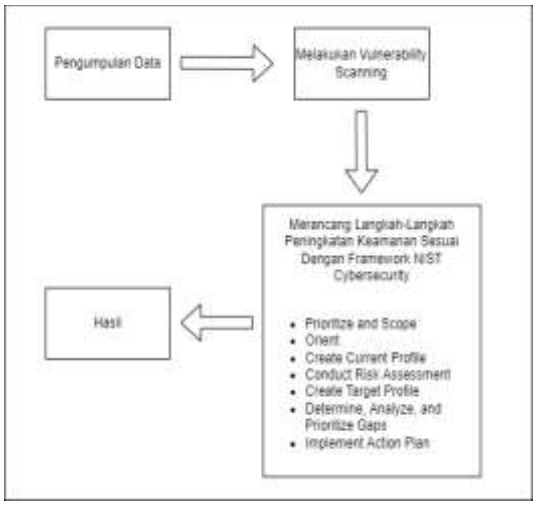
Nessus merupakan tools yang digunakan untuk melakukan evaluasi terhadap jaringan dan layanan berbasistem sistem informasi yang disediakan. Tools ini dapat dijalan dengan menggunakan 1 komputer saja dalam jaringan yang terhubung ke jaringan. Pada tools ini terdapat beberapa fungsi yang dapat digunakan yaitu Vulenerability Sccaing, Configuration Editing, Compliance Checks dan lain-lain[9][10]. Cara kerja dari tools ini adalah melakukan analisa atau network scanning dan melakukan analisa terhadap protokol yang tersedia didalam jaringan. Selanjutnya tools ini akan melalukan analisa dan pengujian untuk menemukan potensi ancaman yang dapat terjadi pada sistem dan teknologi informasi. Pada proses pengujian Nessus melakukan evaluasi pada 1200 pengujian terhadap 1 layanan atau teknologi informasi. Dengan begitu berbagai potensi bahaya seperti celah keamanan, kelemahan sistem dan lain-lain dapat ditemukan[11].

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

2.9. Metode

Metode yang digunakan untuk meningkatkan keamana siber dapat dilihat pada gambar dibawah ini. Tahap 1 Pengumpulan data, 2. Melakukan Vulnerability Scanning, 3. Merancang langkah-langkah peningkatan keamanan sesuai dengan framework NIST Cybersecurity, 4. Hasil.



Gambar 1. Metodologi Penelitian

1. Pengumpulan Data
   Pada tahap ini akan dilakukan pengumpulan data khususnya pada sistem layanan web dan situs web yang digunakan saat ini, informasi mengenai departemen Biro dan Prodi, profil keamanan siber pada saat ini, profil keamanan siber yang ditargetkan, dan data terkait insiden terjadinya peretasan. Pengumpulan data akan dilakukan dengan 2 cara yaitu melakukan wawancara dan observasi lapangan.
2. Melakukan Vulnerability Scanning
   Pada tahap ini akan dilakukan vulnerability scanning terhadap sistem layanan web dan situs web untuk mendapatkan informasi mengenai kerentanan masing-masing situs layanan web dan situs web.
3. Merancang Langkah-Langkah Peningkatan Keamanan Siber Sesuai Dengan Framework NIST Cybersecurity
   Pada tahap ini akan dilakukan peningkatan keamanan siber sesuai dengan rekomendasi dari Framework NIST Cybersecurity. Terdapat 7 langkah yang direkomendasikan antara lain prioritize and scope, orient, create current profile, conduct risk assessment, create target profile, determine, analyze, and prioritize gaps, dan implement action plan.
4. Hasil
   Pada tahap ini akan ditampilkan hasil langkah rekomendasi untuk meningkatkan keamanan siber.

III. PEMBAHASAN DAN HASIL

3.1. Pengumpulan Data

Berikut ini adalah hasil wawancara dan observasi yang telah dilakukan untuk mendapatkan informasi mengenai sistem layanan web dan situs web, informasi mengenai departement, dan informasi mengenai penilaian atau rating dari setiap sistem layanan web dan situs web yang terdapat pada Universitas ZXC. Dari hasil wawancara dan observasi, Univesitas ZXC memiliki 26 layanan sistem, dan 13 website. Untuk Biro terdapat 12 departemen, dan Prodi sebanyak 12 departemen.

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

3.2. Vulnerability Scanning

Tujuan dari melakukan *vulnerability scanning* adalah untuk mendapatkan data kerentanan pada masing-masing sistem layanan web dan situs web. Berdasarkan hasil penetration testing yang dilakukan pada aplikasi web Nessus, dari 26 sistem layanan web, terdapat 1 sistem layanan web dengan threats level Low, 18 sistem layanan web dengan threats level Medium, 1 sistem layanan web dengan threats level High, dan 6 sistem layanan web dengan threats level None. Dari 13 situs web, 5 situs web dengan threats level Medium, dan 8 situs web dengan threats level Low

3.3. Merancang Langkah-Langkah Peningkatan Keamanan Siber Sesuai Dengan Framework NIST Cybersecurity

3.3.1 Prioritize And Scope

Berdasarkan data yang diperoleh dari hasil observasi dan wawancara, bagian-bagian pada Universitas ZXC dapat didefinisikan terbagi dalam 24 departemen yang terbagi dalam 12 Biro dan Lembaga dan 12 Program Studi baik sarjana maupun magister. Penggunaan sistem yang digunakan oleh masing bagian didefinisikan pada Tabel 1.

Tabel 1. Sistem Layanan Web Dan Situs Web Yang Sering Digunakan

Sistem Layanan Web Dan Situs Web	Nama Departemen	Jumlah Departemen Yang Menggunakan Sistem Dan Situs Web
wo.zxc.ac.id	Seluruh departemen	24
myportal.zxc.ac.id	IT Center, BAAK, Post Graduate, Seluruh Prodi	15
portal.zxc.ac.id	IT Center, BAAK, Post Graduate, Seluruh Prodi	15
daftarsidang.zxc.ac.id	IT Center, BAAK, Post Graduate, Seluruh Prodi	15
elearning.zxc.ac.id	IT Center, BAAK, Post Graduate, Seluruh Prodi	15
sa.zxc.ac.id	IT Center, BPKA, Seluruh Prodi	14
daftarkp.zxc.ac.id	IT Center, BAAK, Prodi Akuntansi, Prodi Manajemen, Prodi Ilmu Hukum, Prodi Pariwisata, Prodi Pendidikan Bahasa Inggris, Prodi Sistem Informasi, Prodi Teknologi Informasi, Prodi Teknik Sipil, Prodi Teknik Elektro, Prodi Arsitektur	12
pa.zxc.ac.id	IT Center, BAAK, Prodi Akuntansi, Prodi Manajemen, Prodi Ilmu Hukum, Prodi Pariwisata, Prodi Pendidikan Bahasa Inggris, Prodi Sistem Informasi, Prodi Teknologi Informasi, Prodi Teknik Sipil, Prodi Teknik Elektro, Prodi Arsitektur	12
mou.zxc.ac.id	IT Center, BAUK, Humas, IRO	4
usm.zxc.ac.id	IT Center, BAAK, Humas	3
cbt.zxc.ac.id	IT Center, BAAK, UCLC	3
eservice.zxc.ac.id	IT Center, BAAK, Post Graduate	3

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

akademik.zxc.ac.id	IT Center, BAAK, Post Graduate	3
seminar.zxc.ac.id	IT Center, BPKA	2
pp.lppm.zxc.ac.id	IT Center, LPPM	2
regiatration.iro.zxc.ac.id	IT Center, IRO	2
baak.zxc.ac.id	IT Center, BAAK	2
simlppm.zxc.ac.id	IT Center, LPPM	2
absen.zxc.ac.id	IT Center, BAUK	2
pendaftaran.zxc.ac.id	IT Center, Humas	2
finansi.zxc.ac.id	IT Center, Finance	2
ak.zxc.ac.id	IT Center, Prodi Akuntasi	2
ar.zxc.ac.id	IT Center, Prodi Arsitektur	2
pbi.zxc.ac.id	IT Center, Prodi Pendidikan Bahasa Inggris	2
mh.zxc.ac.id	IT Center, Prodi Magister Hukum	2
ih.zxc.ac.id	IT Center, Prodi Ilmu Hukum	2
ts.zxc.ac.id	IT Center, Prodi Teknik Sipil	2
te.zxc.ac.id	IT Center, Prodi Teknik Elektro	2
mm.zxc.ac.id	IT Center, Prodi Magister Manajemen	2
mn.zxc.ac.id	IT Center, Prodi Manajemen	2
ti.zxc.ac.id	IT Center, Prodi Teknologi Informasi	2
par.zxc.ac.id	IT Center, Prodi Pariwisata	2
si.zxc.ac.id	IT Center, Prodi Sistem Informasi	2
zxc.ac.id	IT Center, Humas	2
bkd.zxc.ac.id	IT Center	1
lc.zxc.ac.id	IT Center	1
ticket.zxc.ac.id	IT Center	1
kuesioner.zxc.ac.id	IT Center	1
admisi.zxc.ac.id	IT Center	1

3.3.2 Orient

Setelah mengidentifikasi 24 departemen dan aplikasi dan sistem yang digunakan. Secara umum terdapat 26 Sistem dan 16 situs web yang digunakan. Dari segi penggunaan, ada terdapat 8 sistem yang digunakan oleh paling tidak 5 bagian berbeda, 16 sistem yang digunakan antara 2-4 bagian dan 6 sistem yang hanya digunakan oleh 1 bagian saja. Dari segi kategori resiko, terdapat 1 sistem yang high risk, 18 sistem dan 5 situs yang

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

medium risk dan 7 sistem dan 8 situs yang low risk. Prioritas dari rating sistem layanan dihitung dari perkalian dari tingkat penggunaan dengan tingkat kategori resiko. Dalam menentukan pengkategorian sistem dan aplikasi secara resiko, digunakan beberapa kriteria pada tabel 2. Dan pada tabel 3 merupakan tingkat prioritas dari masing-masing sistem layanan web dan situs web.

Tabel 2. Kriteria Tingkat Risiko

No	Kategori	Kriteria
1	High Risk (H) (3)	a. Sistem berhubungan dengan layanan pada mahasiswa, baik mahasiswa baru, alumni maupun mahasiswa aktif, baik nasional maupun internasional b. Sistem berhubungan dengan pelaksanaan kegiatan tridharma pada Universitas ZXC c. Sistem berhubungan dengan akreditasi baik Program Studi maupun Perguruan Tinggi d. Sistem Berhubungan dengan keuangan dan penggajian
2	Medium Risk (M) (2)	a. Sistem berhubungan dengan salah satu kategori dari high risk namun digunakan pada saat musiman b. Sistem berhubungan dengan kegiatan operasional dan maintenance diluar tridharma dan keuangan
3	Low Risk (L) (1)	a. Sistem berhubungan dengan diseminasi informasi ke masyarakat b. Sistem hanya digunakan dalam konteks tertentu saja

Tabel 3. Priority Rating Sistem Layanan Web Dan Situs Web

Sistem Layanan / Situs Web	Penggunaan (H, M, L)	Risk Rating (H, M, L)	Priority Rating Sistem Layanan
Bkd.zxc.ac.id	L	L	1
Seminar.zxc.ac.id	L	M	2
pp.lppm.zxc.ac.id	L	H	3
Mou.zxc.ac.id	L	M	2
Registration.iro.zxc.ac.id	L	M	2
Baak.zxc.ac.id	L	H	3
Wo.zxc.ac.id	H	H	9
Cbt.zxc.ac.id	M	H	6
Usm.zxc.ac.id	L	H	3
Simlppm.zxc.ac.id	L	H	3
Daftarkp.zxc.ac.id	H	H	9
Datarsidang.zxc.ac.id	H	H	9
Absen.zxc.ac.id	L	H	3
Pa.zxc.ac.id	H	H	9
Lc.zxc.ac.id	L	L	1
Elearning.zxc.ac.id	H	H	9
Ticket.zxc.ac.id	L	L	1
Eservice.zxc.ac.id	H	H	9
Sa.zxc.ac.id	H	H	9
Kuesioner.zxc.ac.id	L	L	1
Pendaftaran.zxc.ac.id	L	H	3
Finansi.zxc.ac.id	L	H	3
Admisi.zxc.ac.id	M	H	6
Akademik.zxc.ac.id	L	H	3
Myportal.zxc.ac.id	H	H	9
Portal.zxc.ac.id	H	H	9
Ak.zxc.ac.id	M	L	2
Ar.zxc.ac.id	M	L	2
Pbi.zxc.ac.id	M	L	2
Mh.zxc.ac.id	M	L	2
Ih.zxc.ac.id	M	L	2
Ts.zcx.ac.id	M	L	2
Te.zxc.ac.id	M	L	2
mm.zxc.ac.id	M	L	2
Mn.zxc.ac.id	M	L	2
Ti.zxc.ac.id	M	L	2
Par.zxc.ac.id	M	L	2

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

Si.zxc.ac.id	M	L	2
Zxc.ac.id	M	M	4

3.3.3 Create Current Profile

Pada tahap ini, akan dilakukan pembuatan profil keamanan siber saat ini yang menunjukkan kategori dan sub kategori yang terdapat pada Core Framework yang sudah dicapai pada saat ini. Masing-masing sub kategori akan dilakukan penilaian terhadap penerapan pengamanan cybersecurity sudah tercapai dan sesuai yang diinginkan Universitas. Berikut ini adalah tabel untuk penilaian tingkat pencapaian penerapan keamanan siber.

Tabel 4. Penilaian Dan Skala Tingkat Pencapaian

Abbreviation	Description	% Achieved	Point
N	Not Achieved	0 to 15% achievement	0
P	Partially achieved	>15% to 50% achievement	1
L	Largelly achieved	>50% - 85% achievement	2
F	Fully achieved	>85% - 100% achievement	3

Secara umum, kondisi keamanan siber saat ini pada Universitas ZXC menurut standar NIST Framework tidak begitu baik. Pada fungsi Identify, hanya pada kategori Asset Management (ID.AM) dan Business Environment (ID.BE) yang memiliki hasil identifikasi sub-kategorinya cukup baik, namun untuk kategori Governance (ID.GV), Risk Assessment (ID.RA), Risk Management Strategy (ID.RM) dan Supply Chain Risk Management (ID.SC) kondisinya hanya paling baik berlaku sebagian saja atau bahkan tidak ada bentuk implementasi sama sekali. Demikian juga pada Kategori Protect yang hanya memiliki kondisi yang cukup baik pada bagian Authetication and Access Control (PR.AC) dan Data Security (PR.DS). Untuk kategori Detect, Response dan Recovery, Universitas ZXC memiliki kelemahan yang sangat kentara untuk semua sub kategori. Untuk domain identify, protect, detect, respond dan recover, Universitas ZXC hanya memiliki nilai rata-rata 1.33 dari skala 3. Hasil profil keamanan siber pada Universitas ZXC pada saat ini adalah Partially Achieve dimana masih banyak yang harus dilakukan dalam meningkatan keamanan siber.

3.3.4 Conduct Risk Assessmnt

Setelah mendefinisikan prioritas setiap penggunaan sistem dan situs web dan mendefinisikan kondisi profil Standar NIST Framework pada Universitas ZXC, berikutnya adalah melakukan penilaian resiko. Penilaian resiko ini dilakukan dengan mengidentifikasi celah keamanan (vulnerability) dan mengklasifikasikan masing masing ancaman yang berpotensi untuk menganggu layanan. Tingkat parameter dan juimlah celah digunakan untuk menghitung prioritas prioritas sistem layanan web. Untuk melakukan asesmen risiko dari hasil temuan dari nessus, jumlah kelemhan yang berhasil ditemukan apabila dibawah 7 dikategorikan sebagai ‘Low’, jumlah 7-15 dikategorikan sebagai ‘Medium’ dan diatas 15 dikategorikan sebagai ‘High’. Kategori pada thread level diambil dari hasil nessus yaitu dengan status ‘None’, ‘Low’, ‘Medium’ and ‘High’. Untuk menghitung prioritas hasil asesmen, kami menggunakan kalkulasi yang sama digunakan pada fase orientasi. Namun dikarenakan adalah status ‘none’, maka dikalikan dengan angka 0. Dari 39 sistem layanan web yang diuji terdapat 7 sistem dengan jumlah celah yang ditemukan ada pada kategori High, 8 sistem dengan kategori Medium, dan 24 sistem dengan kategori Low. Sedangkan dari tingkat ancaman terdapat 1 sistem dengan kategori ancaman High, 22 sistem dengan kategori ancaman Medium, 9 sistem dengan kategori ancaman Low, dan 7 sistem dengan kategori ancaman None.

Hasil analisis dari aplikasi Nessus, terdapat vulnerability yang terdeteksi pada sistem layanan. vulnerability dengan kategori High yaitu Apache 2.2.x < 2.2.15 Multiple Vulnerabilities, PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution, Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities, Apache 2.2.x < 2.2.34 Multiple Vulnerabilities, dan PHP < 5.2.11 Multiple Vulnerabilities dengan masing-masing dengan detected count sebanyak 1 kali. Terdapat pula vulnerability yang sering ditemui yaitu SSL Medium Strength Cipher Suites Supported (SWEET32) detected count sebanyak 20 kali dengan kategori vulnerability Medium, SSL RC4 Cipher Suites Supported (Bar Mitzvah) detected count sebanyak 10 kali dengan kategori vulnerability Medium.

Pada Aplikasi Nessus, juga memberikan rekomendasi untuk mencegah terjadinya vulnerability yang telah disebutkan yaitu langkah Preventive:

1.Konfigurasi ulang aplikasi yang terpengaruh jika memungkinkan untuk menghindari penggunaan cipher berkekuatan sedang.

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022

2.Konfigurasi ulang aplikasi yang terpengaruh, jika memungkinkan, untuk menghindari penggunaan cipher RC4. Pertimbangkan untuk menggunakan TLS 1.2 dengan suite AES-GCM yang tunduk pada dukungan browser dan server web.
3.Tingkatkan ke JQuery versi 3.5.0 atau lebih baru.
4.Tingkatkan ke Apache versi 2.2.15 atau yang lebih baru.
5.Tingkatkan ke PHP versi 5.2.11 atau lebih baru.

Mitigasi:
1.Data Recovery menggunakan data backup
2.Melakukan vulnerability analysis
3.Patching system

3.3.5 Create Target Profile

Setelah mengetahui kondisi awal pada Universitas ZXC dan melakukan asesmen terhadap risiko yang ada, maka selanjutnya dilakukan penilaian untuk menentukan target profile. Target Profile adalah sasaran yang ingin dicapai oleh Universitas ZXC sesuai dengan standar NIST Framework. Profil yang ditargetkan Universitas dalam peningkatan keamanan siber yaitu sebesar 2 dari skala tiga yaitu Largely Achieve.

3.3.6 Determine, Analyze, And Prioritize Gaps

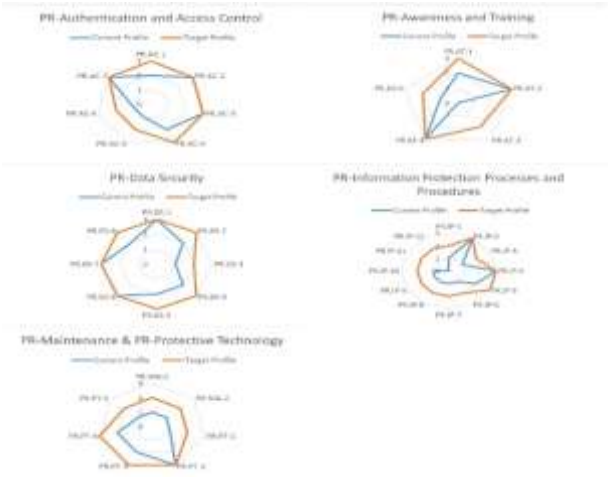
Hasil dari analisa gap dapat dilihat pada gambar dibawah ini. Pada Identify-Asset Management, tidak terlalu banyak perubahan yang dilakukan kecuali pada ID-AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established yang dari posisi N (0) menuju ke L (2). Demikian pula pada kategori Identify-Business Environment yang sudah kondisinya sesuai dengan Standar NIST Framework. Untuk Kategori lain, seperti Governance, Risk Assessment, Risk Management Strategy dan Supply Chain Risk Management, terdapat perubahan yang cukup signifikan.

Gambar 2. Gap Pada Kategori Identify

Pada Kategori Protect, sub kategori yang mengalami target perubahan yang drastis adalah PR-AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities dan PR-IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). Beberapa sub-kategori sudah mencapai target yang diharapkan seperti PR-AC-2, PR-AC-3, PR-AC-7, PR-AT-2, PR-AT-4, PR-DS-1, PR-DS-6, PR-DS-7, PR-AP-1, PR-IP-4 dan PR-PT-2. Secara umum terdapat target peningkatan untuk kategori Protect di Universitas ZXC.

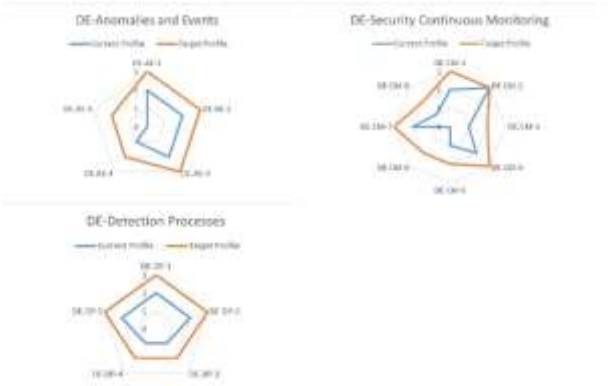
DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022



Gambar 3. Gap Pada Kategori Protect

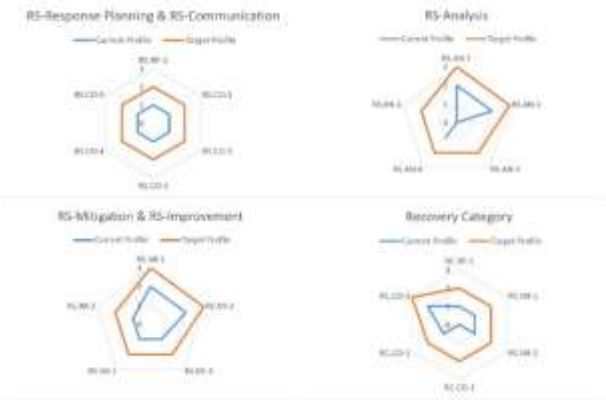
Pada kategori Detect, dimana Universitas ZXC mengalami kondisi yang paling tidak sesuai dengan standar NIST Framework, terdapat sasaran peningkatan yang meningkat. Kondisi ini juga terjadi pada kategori Response dan Recovery.



Gambar 4. Gap Pada Kategori Detect

DOI: 10.52362/jisamar.v6i2.781

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.2 May 2022



Gambar 5. Gap Pada Kategori Respon Dan Recovery

3.3.7 Implement Action Plan

Kondisi awal Universitas ZXC telah dianalisis oleh penulis dari segi semua kelemahan yang terdeteksi pada layanan sistem dan situs web. Dari kelemahan yang berhasil diidentifikasi, kemudian penulis merangkum resiko yang mungkin terjadi. Kebijakan dan prosedur yang telah berlaku di lingkungan Universitas ZXC kemudian dikombinasikan dengan tindakan rekomendasi penulis untuk memenuhi gap yang ada antara kondisi sekarang dengan kondisi sasaran. Kepatuhan terhadap standar NIST Framework yang dicapai dengan tindakan yang penulis rekomendasi untuk dijalankan perlu mendapat persetujuan dari manajemen Universitas ZXC. Oleh karena itu, penulis akan menyerahkan sepenuhnya kepada pihak manajemen apakah rekomendasi diterima dan dilanjutkan dengan program kerja atau tidak.

IV. KESIMPULAN

Dengan menggunakan Framework NIST Cybersecurity, Universitas ZXC terbantu dalam penilaian keamanan siber pada saat ini. Framework ini juga sangat cocok untuk digunakan karena nantinya bisa menyesuaikan perubahan dan perkembangan teknologi kedepannya. Tidak hanya untuk Universitas ZXC, rekomendasi menggunakan Framework NIST Cybersecurity juga bisa digunakan pada tempat yang lain khususnya pada Universitas.

REFERENSI

[1] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, “Mobile Application Security Penetration Testing Based on OWASP,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 846, no. 1, 2020, doi: 10.1088/1757-899X/846/1/012036.

[2] A. Kohnke, K. Sigler, and D. Shoemaker, *Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework*. 2017.

[3] U. M. Mbanaso, L. Abrahams, and O. Z. Apene, “Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework,” *African J. Inf. Commun.*, no. 23, pp. 1–26, 2019, doi: 10.23962/10539/27535.

[4] M. Benz and D. Chatterjee, “Calculated risk? A cybersecurity evaluation tool for SMEs,” *Bus. Horiz.*, vol. 63, no. 4, pp. 531–540, 2020, doi: 10.1016/j.bushor.2020.03.010.

[5] J. Webb and D. Hume, “Campus IoT collaboration and governance using the NIST cybersecurity framework,” *IET Conf. Publ.*, vol. 2018, no. CP740, pp. 1–7, 2018, doi: 10.1049/cp.2018.0025.

DOI: 10.52362/jisamar.v6i2.781

[6] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–8, 2020, doi: 10.1093/cybsec/tyaa005.

[7] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, vol. 4, no. 10, pp. 13–21, 2014, doi: 10.22215/timreview835.

[8] T. Mauritsius and B. A. Saputra, "Enhancing cybersecurity on private cloud using nist cybersecurity framework," *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 15, pp. 4159–4174, 2019.

[9] S. E. Prasetyo and R. C. Lee, "Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing," *Tek. Inform.*, vol. 1, no. 1, pp. 710–718, 2021.

[10] S. Noel, M. Elder, S. Jajodia, P. Kalapa, S. O'Hare, and K. Prole, "Advances in topological vulnerability analysis," *Proc. - Cybersecurity Appl. Technol. Conf. Homel. Secur. CATCH 2009*, no. June 2014, pp. 124–129, 2009, doi: 10.1109/CATCH.2009.19.

[11] Tenable, "NESSUS IS #1 FOR VULNERABILITY ASSESSMENT," 2021. .

DOI: 10.52362/jisamar.v6i2.781